

REMARKS/ARGUMENTS

In view of both the amendments presented above and the following discussion, the applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 USC §§ 102 and 103. Furthermore, the applicants also submit that all of these claims now satisfy the requirements of 35 USC § 112. Thus, the applicants believe that all of these claims are now in allowable form.

If the Examiner believes that there are any unresolved issues in any of the claims now pending in the application, the Examiner is urged to telephone Ms. Alberta A. Vitale, Esq. at (203) 469-8097 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Specification Amendments

The specification has been amended to correct minor typographical errors. Additionally, the specification has been amended to properly format trademark references in as required by MPEP §608.01(v). A copyright notice has been added in conformance with MPEP §608.01(v).

Claim Amendments

No amendments have been made to the claims. No claims have been added or cancelled.

Rejections under 35 U.S.C. § 103

1. § 103 Haung in view of Zhu in view of Burgess

The Office action, at paragraph 3, has rejected claims 1-4, 8, 10-17, 21,23-27, 31, 33-40, 44 and 46 under the provisions of 35 USC § 103 as being obvious over the teachings in the Haung patent (United States patent 6,571,245 issued to Erwin S. Haung et al on May 27, 2003 (hereinafter Haung)) taken in view of the Zhu patent (United States patent 6,691,154 issued to Min Zhu et al on February 10, 2004 (hereinafter Zhu) and further in view of the Burgess patent (United States patent 5,796,633) issued to Gregory M. Burgess et al on August 28, 1998 (hereinafter Burgess)).

These rejections are respectfully traversed. For simplification, the Applicants will specifically discuss these rejections in the context of independent claims 1 and 24 from which claims 2-23 and 25-36 depend, respectively.

Since claim 1 (apparatus) and claim 24 (method) contain highly similar limitations, and since the Office action recites the same rejection, including citations to

the art, for claim 24 as for claim 1, Applicants will discuss the rejections with respect to claim 1.

Claim 1

Claim 1 is recited as follows:

Apparatus for monitoring a local area network (LAN) through a remote administrative web site, the apparatus comprising:

a service enablement platform (SEP) for connection to the LAN and for connection, through a wide area network (WAN) connection, to the administrative web site, wherein the SEP comprises:

a processor;

a memory, connected to the processor, for storing computer executable instructions therein; and

first and second network interfaces, operable in conjunction with the processor, for communicatively interfacing the SEP, through a first network connection, to the WAN and, through a second network connection, to the LAN, respectively;

wherein the processor, in response to execution of the instructions:

continually monitors operational status of a monitored entity so as to detect an alarm condition resulting from an operational failure in the monitored entity, the monitored entity comprising the SEP, at least one of the first and second connections or at least one of a plurality of servers residing on the LAN;

generates, in response to the alarm condition, an alarm message containing information related to the alarm condition;

converts the alarm message into a predefined format suitable for communication over a web connection so as to yield a web-communicable alarm message; and

transmits the web-communicable alarm message, via the WAN interface and the first network connection, to the administrative web site which, in response to receipt of the web-communicable alarm message:

extracts the alarm information from the web-communicable alarm message so as to define extracted alarm information; and

updates a record in a database, maintained by the administrative web site and associated with the SEP, to reflect the extracted alarm information. (emphasis added).

The Office Action at paragraph 4, page 2 states that "Haung Figure 2, 230 site server provides link and col. 4, lines 47-49" teaches "a service enablement platform (SEP) for connection to the LAN and for connection, through a wide area network (WAN) connection, to the administrative web site." (emphasis added). Applicants note that the citation of Haung, col. 4, lines 47-49, states: "Site server 230 further couples to a bus 244 that interconnects one or more regional networks 250. Each regional network 250 supports a particular geographic area." (emphasis added). The Office action further cites Figure 2, reference numeral 230 "site server".

However, Applicants respectfully note that neither Figure 2, nor the above quoted citation makes any reference to Applicants' claimed "platform" (claim 1, clause 1, emphasis added). Nor, for that matter is platform described anywhere in Haung, cited or not. It appears that the Office action is using the citation to show a teaching of networks and servers. Nowhere in the citation is their any teaching of Applicants' platform or SEP (Service Enablement Platform), which is described at length in the

specification and is illustrated in Figure 1 (200) and Figure 2 (high-level block diagram of SEP 200).

Applicants' specification states:

In accordance with our inventive teachings and as described in considerable detail below, SEP 200 provides a front end to server 70 for implementing secure, remote, web-based access, through browser 15, by a user situated at client 10 to the network-based office functionality implemented by server 70 and to the same extent as if client PC 10 were directly connected to LAN 65. Server 70 resides on LAN 65 to collectively implement, through separate internal LAN accessible application servers, various office processing applications (tasks) including, through client applications server 72, thin-client hosted application programs; through web-enabled application server 74, remotely-hosted web-enabled thin-client application programs; through e-mail server 76, e-mail messaging; and, through file

server 78, shared file access."

(Page 35, line 26 to page 36, line 13;
emphasis added).

Furthermore, Applicants' "platform" is claimed as "having:" "a processor", "a memory ... first and second network interfaces ..." and functionality described in the detailed wherein clause emphasized in-part in the above claim 1. While the Office action has made an attempt to show that the various aspects of the claimed apparatus are taught by Haung in view of Zhu and further in view of Burgess, Applicants respectfully disagree with the Office action because those aspects of the apparatus are cited in a piecemeal format that does not provide any teaching, suggestion or motivation for Applicants' claimed invention. Applicants further explain below.

Firstly, the Office action attempts to show a teaching of Applicants' "processor" by citing to Haung at "col. 4, lines 47-49", "memory" by citing to Haung at "Figure 15 and col. 18, line 62 to col. 19, lines 20", and network interfaces and network connection by citing to Haung at "Figure 2, col. 4, lines 26-40" and "Figure 2 and column 1, lines 40-47, column 4, lines 47-67 and column 5, lines 35-54) respectively. These citations (as well as other citations) and any corresponding explanations in the Office action ignore that each of these elements are

part of Applicants' "service enablement platform (SEP) ... wherein the SEP comprises a processor" with functionality "wherein the processor, in response to execution of instructions ... monitors ... generates ... converts ... transmits ... extracts ... and updates." (Claim 1, wherein clause, emphasis added).

The Office action further states, at page 4, para. 5, that essentially Haung fails to teach "service enablement platform (SEP) ... wherein the SEP comprises a processor" with functionality "wherein the processor, in response to execution of instructions ... monitors ... generates ... converts ... transmits ... extracts ... and updates." (Claim 1, wherein clause, emphasis added). The Office action goes on to cite Zhu as teaching these functions.

At paragraph 6 pages 4-5, the Office action states:

However, Zhu et al teach monitoring operational status of a monitored entity so as to alarm condition resulting from an operational failure in the monitored entity (column 3, lines 38-40), at least one of the first and second connections or at least one of a plurality of servers residing on the LAN (column 3, lines 38-40; local unattended server); generates, in response to the alarm

condition, an alarm message containing information related to the alarm condition (column 3, lines 41-45); converts the alarm message into a predefined format suitable for communication over a web connection so as to yield a web-communicable alarm message (column 3, lines 41-58); and transmits the web-communicable alarm message, via the WAN interface and the first network connection (column 3, lines 9-13; internet browser and column 3, lines 50-58), to the administrative web site which, in response to receipt of the web-communicable alarm message: extracts the alarm information from the web-communicable alarm message so as to define extracted alarm information (column 3, lines 40-45 and lines 59-67)). (emphasis added).

Applicants reviewed the above Zhu citations, summarizing the citations and the remarks and providing a response as follows regarding the citation to:

1) "Monitoring", "server", "(column 3, lines 38-40 and local unattended server)", the cited portion of Zhu states: "The monitoring application 130 monitors the status of one or more applications running on the local unattended

server 104." (col. 3, lines 38-40, emphasis added). Applicants respectfully note that Applicants' claimed "processor ... monitors operational status ... to detect an alarm condition." (emphasis added). The only similarity between Applicants' "status" and Zhu's "status" is that they are named similarly. Similarity in nomenclature is not enough to provide teaching of Applicants' claim element or claimed invention. Zhu clearly does not teach what is claimed.

2) "Generates", "(column 3, lines 41-45") the cited portion of Zhu states: "Methods for monitoring applications are well known in the relevant arts. The monitoring application 130 can be configured to generate and send an event flag identifying a running application that may require external support to the remote conferencing server 102." (col. 3, lines 41-45, emphasis added). Applicants respectfully note that Applicants' claimed "processor ... generates in response to the alarm condition, an alarm message containing information related to the alarm condition." (emphasis added). Since Zhu's "an event flag" is not the same as Applicants' "alarm condition" and Zhu's "event flag" provides not teaching or suggestion of Applicants' "alarm condition" in the context of the claimed

invention, Zhu clearly does not teach what is claimed.

3) "Converts", "(column 3, lines 41-58)" the cited portion of Zhu states: "The monitoring application 130 can be configured to generate and send an event flag identifying a running application that may require external support to the remote conferencing server 102. The local document sharing application can include a communication module 134 and a document loader 136. The document loader can have an application invoker 138 and virtual devices and drivers 140. The functions of these elements will be described in greater detail below. In one implementation, the remote conferencing server 102 uses communications protocols, such as the H.323 protocols and the T.120 protocols (established by the International Telecommunications Union), to provide support for real-time, multipoint data communications across IP-based networks, including the Internet. The remote conferencing server 102 can establish a data conference that enables collaboration, such as application sharing and document sharing, between multiple remote experts 106." (col. 3, lines 41-58, emphasis added). Applicants respectfully note that Applicants' claimed instruction "converts the alarm message ... to

yield a web-communicable alarm message" (emphasis added) whereas Zhu is discussing event flag and communications protocols. This is clearly not the same as "web-communicable alarm". This is further described in Applicants' specification as follows:

Additionally, the SEP continually monitors operational status of itself including its network (LAN and WAN) connections, LAN-connected servers including, for example, each of the hosted office application servers, and/or any group thereof. In the event of a detected fault or failure condition in any monitored entity, the SEP generates a corresponding alarm and reports it, through a web-based connection, to a centralized administrative web site (referred to herein as a "Customer Care Center" (CCC)) to implement remote network monitoring and management functionality. This functionality is implemented through converting data content, including alarm information, from a native format into HTTP-based messaging with the latter being used for web transport and converting that

content, once received at the CCC, into an appropriate format for storage thereat. Advantageously, this web-based reporting technique readily allows a large number of separate LANs that are dispersed over a very wide geographic area to be readily monitored and managed through the CCC. Moreover, the number of such managed networks can be easily scaled upward, as needed, by, for the most part, simply and correspondingly expanding processing and storage capacity of the CCC to handle the anticipated load.

(Specification at page 21, line 11 to page 22, line 7, emphasis added).

4) "Transmits", "(column 3, lines 9-13; internet browser and column 3, lines 50-58)" the cited portions of Zhu state: "Each remote expert 106 includes an operating system 108, a memory 110, and a remote document sharing application 114. In one implementation, the remote expert 106 is a computer running a Windows-type operating system (OS) that has a web browser such as Windows Internet explorer."

(col. 3, lines 9-13, emphasis added) and "In one implementation, the remote conferencing server 102 uses communications protocols, such as

the H.323 protocols and the T.120 protocols (established by the International Telecommunications Union), to provide support for real-time, multipoint data communications across IP-based networks, including the Internet. The remote conferencing server 102 can establish a data conference that enables collaboration, such as application sharing and document sharing, between multiple remote experts 106." (col. 3, lines 50-58). Applicants' claim language states "the processor, in response to execution of the instructions: transmits ... the web-communicable alarm message, via WAN interface ... to the administrative website, which in response to receipt of web-communicable alarm message." Applicants' respectfully note that the only hint of similarity between the citation and the claim language is the use of "web browser" by Zhu and Applicants' "web-communicable". However, this nomenclature in no way implies that Zhu teaches Applicants' web-communicable in the context of the claimed invention. Therefore, Applicants assert that there is no teaching of the claimed invention by Zhu.

6) "Extracts", "(column 3, lines 40-45 and lines 59-67))" the cited portions of Zhu state: "The monitoring application 130 monitors the status of one or more applications running on the

local unattended server 104. Methods for monitoring applications are well known in the relevant arts. The monitoring application 130 can be configured to generate and send an event flag identifying a running application that may require external support to the remote conferencing server 102." (col. 3, lines 40-45) and "Referring to FIGS. 1 and 4a, the remote conferencing server 102 can automatically establish a data conference (step 402) upon receipt of the event flag and send information regarding the data conference to the local unattended server 104, which uses the information to join the data conference (step 404). The remote conferencing server 102 then notifies select remote experts 106 that a data conference of interest has been established and allows only the select remote experts 106 to join the data conference (step 404). Alternatively, the remote conferencing server 102 notifies all the remote experts 106 that the data conference has been established. In this implementation, the remote experts 106 have to monitor the list of data conferences on the remote conferencing server 102 and select the data conference to join (step 404)." (col. 3, lines 59-67, emphasis added). Applicants' claimed "extracts alarm information ... so as to define extracted alarm information" is not taught by the Zhu citations.

Zhu's "establishes ... a data conference upon receipt of event flag" does not teach and is not Applicants' "extracts alarm information from the web-communicable alarm message so as to define extracted alarm information."

Applicants' specification further details alarm information as follows:

"FIG. 25 depicts inter-process communication that occurs, in response to an alarm generated within SEP 200, for providing alarm information from the SEP to web site 20" (Specification, page 30, lines 16-19, emphasis added) and "If the message is authentic, then the transport layer extracts the de-serialized XML, converts it to a WDDX hash structure therefrom and applies that structure to CC_RMM_RECEIVE module 2232 which, specifically through its WDDX translation module 2233 (see FIG. 22), converts the WDDX hash structure containing the alarm information into Perl data. In response to this request, module 2232 then writes, through operation 2535 and as symbolized by line 2540, the alarm information into CCC

database 1980." (Specification, page 119,
line 25 to page 120, line 6, emphasis
added).

The Office action, at page 4, paragraphs 7 and 8, further states that "Huang et al fail to teach updating a record in a database, maintained by the administrative web site and associated with the SEP, to reflect the extracted alarm information ... However, Burgess et al teach updating performance data recorded in a central database on a second computer coupled to the computer network after an alert has been generated once the performance level has reached an alterable level (abstract and column 2, lines 35-45)." (emphasis added). The cited portions of Burgess are repeated as follows:

The invention comprises a method and system for monitoring the performance of a computer coupled to a computer network and, optionally, generating alerts when the performance of the computer has reached an alertable level. The method of monitoring the performance of the computer comprises repeatedly obtaining performance data using the computer wherein at least one performance value comprises a measure of the performance of the computer. The performance data is automatically sent over the computer network to a second computer coupled to the computer network. The performance data is then

logged to a performance database using the second computer.

(Burgess Abstract, emphasis added).

The invention has several important technical advantages. The invention allows performance monitoring of computers in a computer network to be handled automatically without human intervention. The invention allows recording of performance data in a central database, providing network planners with a tool to analyze the historical performance of computers in the computer network as well as the performance of the network itself. In addition, network planners may use the database to monitor usage trends among various computers connected to the computer network.

(Burgess, column 2, lines 35-45, emphasis added).
Clearly, neither of these citations to Burgess teach Applicants' claimed "updating a record in a database, maintained by the administrative web site and associated with the SEP, to reflect the extracted alarm information". (emphasis added).

Applicants respectfully remind the Examiner that obviousness cannot be made piecemeal. That is, the Examiner cannot attempt to piece together the

claimed invention using the claims as a guide. "It is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious 'one cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention.'" *In re Fritch*, 972 F.2d 1260, 23 USPQ2d 1780, 1784 (Fed. Cir. 1992) (quoting *In re Fine*, 837 F.2d 1071, 1075, 5 USPQ2d 1596, 1600 (Fed. Cir. 1988)).

Furthermore, Applicants' note that there is no teaching, suggestion or motivation to combine Huang in view of Zhu in view of Burgess. Huang is directed to "a template for providing a virtual desktop in a computer network" (col. 1, lines 11-12), Zhu is directed to "initiating a desktop controlling session of an unattended server from a remote site" and Burgess is directed to "a method and system for monitoring the performance of a computer in a computer network" whereas Applicants' invention is directed to "apparatus and accompanying methods for use therein for implementing a secure, cost-effective, web-enabled, integrated, virtual office user environment, through a centralized server(s), through which a remotely stationed user can access typical office network-based applications, including, e.g., e-mail, file sharing and hosted thin-client application programs, through a remotely located network, e.g., WAN, connected

web browser, as well as for remotely providing network monitoring and management capabilities through a centralized administrative web site." The mere similarity of various nomenclature or terms used in Haung, Zhu or Burgess is not enough to make Applicants claimed invention obvious.

For all of the above stated reasons, Applicants respectfully request that the 35 USC § 103 rejection of claim 1 be withdrawn.

Claim 24

For all of the above stated reasons with respect to claim 1, claim 24 is not obvious and Applicants respectfully request that claim 24 be allowed.

Claims 2-23 and 25-46

Claims 2-23 depend from independent claim 1, and claims 25-46 depend from independent claim 24. For all of the above stated reasons, Applicants respectfully note that the dependent claims are not obvious and request that they be allowed.

Further, with respect to claims 2-10, 13, 14, Applicants will address the remarks of the Office action individually below.

Claim 2

Claim 2, depends from independent claims 1 and recites: "The apparatus in claim 1 wherein the processor, in response to execution of the stored instructions: forms an HTTP message containing the alarm information; and encrypts the HTTP message to form the web-communicable message." (emphasis added). The Office action, at page 5, paragraphs 10-11, states that: "As per claim 2, Huang et al fails to teach forming an HTTP message containing the alarm information; and encrypts the HTTP message to form the web-communicable message However, Zhu et al teach a remote expert using Windows Internet Explorer can view a flag that contains information regarding the status of a monitored server and can (column 3, lines 9-13 and column 3, lines 38 - 45). It would have been obvious to one of the ordinary skill in the art ... combine the teachings of Zhu et al and Burgess et al to Huang et al's apparatus because Zhu et al's use of a monitoring application status and event flags to identify alarm conditions and use of HTTP messages with Burgess et al's use of a database in Huang et al's apparatus would allow for a monitoring entity to view and receive status information regarding monitored computers using a web browser and store this information in a database for future references."

Applicants recite the full text of the citations to Zhu as follows:

Each remote expert 106 includes an operating system 108, a memory 110, and a remote document sharing application 114. In one implementation, the remote expert 106 is a computer running a Windows-type operating system (OS) that has a web browser such as Windows Internet explorer. (col. 3, lines 9-13).

The monitoring application 130 monitors the status of one or more applications running on the local unattended server 104. Methods for monitoring applications are well known in the relevant arts. The monitoring application 130 can be configured to generate and send an event flag identifying a running application that may require external support to the remote conferencing server 102. (col. 3, lines 38-45).

While the Zhu citation discusses "an event flag identifying a running application" this is far from providing any teaching or suggestion of Applicants' claimed "wherein the processor, in response to execution of the stored instructions: forms an HTTP message containing the alarm information; and encrypts the HTTP message to form the web-communicable message." (Claim 2, emphasis added). Furthermore, claim 2, which depends from claim 1 is further not obvious for reasons discussed above with respect to

claim 1. Therefore, Applicants respectfully request that the rejection be withdrawn.

Claim 3

Claim 3, depends from claims 2 and recites: "The apparatus in claim 2 wherein the SEP further comprises a web client executed by the processor and the administrative web site comprises a web server with the HTTP message being transported, via the WAN and over a web connection, from the web client to the web server." The Office action, at page 4, paragraph 12, states that: "As per claim 3, Huang et al teach a web client executed by the processor (Figure 2; 210, Figure 3 and Figure 4) and the administrative web site comprises a web server (Figure 2; site server) with the HTTP message being transported, via the WAN and over a web connection, from the web client to the web server (Figure 4; and column 7, lines 11-32)."
Applicants have reviewed the references to the Figures and the citation to col. 7, lines 11-32, which is repeated as follows for convenience:

FIG. 4 shows, in summary form, some of the processes and features provided by the virtual desktop of the invention. As shown in FIG. 4, the web page from the site server initially includes a login window 410 that prompts the user for an identification and a password. The user then enters the requested information in the

appropriate fields. Upon indicating that the information has been entered (i.e., by hitting the carriage return in the password field), a secured transaction 412 is initiated with URL site server 230. The login information is securely transmitted to site server 230 using, for example, a Secured Socket Layer (SSL) based security technique. Site server 230 determines whether the user is registered and, if yes, transmits the user's personal web page. The login process is described in further detail below.

After a successful login, the user's personalized virtual desktop 420 is transmitted, received, and displayed. Desktop 420 corresponds generally to browser display 300 in FIG. 3. The user can then activate the features of the virtual computer by activating the appropriate icon from virtual desktop 420. In general, through virtual desktop 420, the user has access to applications, files, news and information, and additional features.

Applicants' fail to see where in the above citation their claimed "SEP further comprises a web client executed by the processor and the administrative web site comprises a web server with the HTTP message being transported, via the WAN and over a web connection, from the web client to the web

server." Applicants respectfully remind the Examiner that a rejection must be "clearly articulated" (as is required by § MPEP 706) and that even assuming arguendo this aspect of claim 3 were taught or disclosed by the Haung citation, obviousness cannot be made "piecemeal" as is discussed supra. Furthermore, Claim 3, which depends from claim 2 and indirectly from claim 1 is further not obvious for reasons discussed above with respect to each of claims 1 and 2. Therefore, Applicants respectfully request that the rejection be withdrawn.

Claim 4

Claim 4, depends from claims 2 and recites: "The apparatus in claim 2 wherein the processor, in response to execution of the stored instructions, signs the HTTP message using a private key associated with the SEP prior to encrypting the HTTP message." The Office action, at page 6, paragraph 13, states that: "As per claim 4, Huang et al teach signing the HTTP message using a private key associated with the SEP prior to encrypting the HTTP message (column 15, lines 12-59 and 45-64)." The cited portions of Haung are repeated as follows

Once logged in, the user is granted access to the user's virtual desktop. As shown in FIG. 2, firewall 232 exists between the Internet 210 and site server 230. Firewall 232 supports transactions that use HTTP/FTP protocol. As a

choice, the user is allowed to select encryption for the login process only, or encryption for the entire session. Thus, during an active session, the transactions can be secured or unsecured, which is indicated by dashed lines for transactions 1222. If full encryption is selected, each transaction between the local PC and the site server is a secured process. Full encryption may slow down the communications between the local PC and the site server because of the extra encryption processing, but provides a secured computing environment. Additionally, a virus check can be performed on files before the upload (and download) from the local PC to the network.

To terminate the session, the user logs out by clicking on a logout (LO) icon 1232 on a virtual desktop 1230. The logout command is sent to servers 1216. In an embodiment, as part of the logout process, servers 1216 execute (or direct execution) of a termination application 1240 which clears the RAM on the local PC 1250 and the hard dish cache so that "ghost" copies of files are destroyed upon termination of the session. Termination application 1240 can reside on the local PC (i.e., as part of the local PC operating system) that is activated by servers 1216.

Virtual Desktop Processes

FIGS. 13A and 13B show a flow diagram that describes an implementation of an embodiment of the virtual desktop of the invention. The flow diagram describes implementation of some of the features recited above. Thus, FIGS. 13A and 13B should only be taken as representative, and not limitation, of the invention.

In FIG. 13A, at a step 1310, the URL website that supports the virtual desktop receives a URL access from one of the local PC. In response, the URL sends its web page and a login window, at a step 1312. Shortly thereafter, the URL receives, at a step 1314, the login information and compares, at a step 1316, the received login information with the login information stored at the URL for that user. At a step 1318, a determination is made whether the received login information is valid. If the received login information is not valid, an error message is sent to the local PC, at a step 1320, the login window is redisplayed, at a step 1322 (i.e., with the previously entered data removed from the login window fields), and the site server returns to step 1312.

(column 15, lines 12-59, emphasis added).

In FIG. 13A, at a step 1310, the URL website that supports the virtual desktop receives a URL access from one of the local PC. In response, the URL sends its web page and a login window, at a step 1312. Shortly thereafter, the URL receives, at a step 1314, the login information and compares, at a step 1316, the received login information with the login information stored at the URL for that user. At a step 1318, a determination is made whether the received login information is valid. If the received login information is not valid, an error message is sent to the local PC, at a step 1320, the login window is redisplayed, at a step 1322 (i.e., with the previously entered data removed from the login window fields), and the site server returns to step 1312.

If the login is valid, the session starts at a step 1330. The site server then directs one of the backend server to handle the session with the user. The security mode (e.g., no encryption, partial encryption, or full encryption), as selected by the user or the server, is then set by the server, at a step 1332.

(column 15, lines 45-64, emphasis added). Nowhere in the above citation is there any teaching or suggestion of

Applicants' claimed "processor" or Applicants' processor "signs the HTTP message using a private key associated with the SEP prior to encrypting the HTTP message." Again, Applicants' note that obvious cannot be made "piecemeal" (see remarks supra). Additionally, even assuming arguendo that the remarks were not made in a piecemeal format, there is no teaching of Applicants' processor in the context of the claimed invention. Nor is there any teaching of signature using "private key associated with the SEP." Nor is there any teaching of "private key". Applicants respectfully note that Haung's encryption does not teach or suggest Applicants' use of "private key" in the context of the claimed invention. Applicants further explain their encryption in the specification at page 23, line 1 to page 25, line 7, repeated as follows:

Moreover, during initial installation of the SEP at any customer site, the SEP, after being connected to analog (dial-up) and broadband WAN connections, will dial the CCC and establish a management session with it, through use of a predefined default profile that provides access information to the CCC, in order to obtain appropriate customer WAN login parameters therefrom. The SEP will identify itself to the CCC by providing its hardware media access code (MAC) address and will authenticate itself using HTTP authentication. Specifically, the SEP will identify itself via its MAC address to the CCC.

The CCC will issue a challenge value to the SEP. The SEP will encrypt the challenge value using its private key (of the public key/private key pair stored within the SEP) and respond with the encrypted value. In turn, the CCC will decrypt the response from the SEP. If a resulting value matches the challenge value, the CCC will then consider the SEP to be successfully authenticated. Once a management session has been established with the CCC, the CCC will send the SEP appropriate login and password for a customer WAN account which that the SEP is to use. On receipt of the customer's WAN account information from the CCC, the SEP will tear down its existing analog call to the WAN in order to minimize the length of these initial calls. The SEP will then establish a broadband connection to the WAN service provider using the customer's WAN account information. Once a WAN login succeeds, the SEP will continue with its previous management session, though secured through SSL, with the CCC. The SEP will then interact with the CCC and obtain a valid client certificate from the CCC. Future interactions between the CCC and SEP will use the client certificate to authenticate this SEP in lieu of the previously-used challenge/response mechanism.

In addition to obtaining its client certificate from the CCC during a remainder of the management session, the SEP will also download its customized profile from the CCC. After successfully obtaining this profile, the SEP will terminate the SSL session between itself and the CCC, reset itself, and then re-initialize itself using the customized profile to correctly configure its various constituent hardware components and software modules to its current environment. Once correct information identifying the customer is then entered by an administrator at the SEP -- with the information matching that in the customized profile, the SEP will enter a fully operational mode and accordingly will send an appropriate management message to the CCC to indicate that the SEP is then fully operational.

In accordance with a feature of our invention, while the principal office-based applications are file sharing, e-mail and thin-client application program hosting, our invention can readily and easily accommodate web-based, secure, remote user access to other additional office-based applications by merely incorporating a corresponding client application module for each such additional office application to provide required bi-directional, real-time protocol

translation for both incoming user interaction data to that office application and output data generated by that office application.

(emphasis added). For the above noted reasons, Applicants' claim 4 is clearly not taught by the references. Furthermore, Claim 4, which depends from claim 2 and indirectly from claim 1 is further not obvious for reasons discussed above with respect to each of claims 1 and 2. Therefore, Applicants respectfully request that the rejection be withdrawn.

Claim 8

Claim 8, depends from claims 4 (and indirectly from claim 1) and recites: "The apparatus in claim 4 wherein the administrative web site in response to receiving the HTTP message: decrypts the HTTP message so as to define a decrypted HTTP message; authenticates the decrypted HTTP message using a signature contained within HTTP message; and if the decrypted HTTP message is authentic, updates the record in the database in response to the alarm information carried in decrypted HTTP message." The Office Action at page 6, paragraph 13 states "As per claim 8, Huang et al teach decryption of the HTTP message so as to define a decrypted HTTP message (column 15, lines 12-59); authenticates the decrypted HTTP message using a signature contained within HTTP message (column 15, lines 12-59 and 45-64); and if the decrypted

HTTP message is authentic (column 15, lines 12-59 and lines 45-64), updates the record in the database in response to alarm information carried in decrypted HTTP message (Figure 13A and column 15, line 59 - 66; information can be of any type)."

The citations to Haung are repeated as follows for convenience:

Once logged in, the user is granted access to the user's virtual desktop. As shown in FIG. 2, firewall 232 exists between the Internet 210 and site server 230. Firewall 232 supports transactions that use HTTP/FTP protocol. As a choice, the user is allowed to select encryption for the login process only, or encryption for the entire session. Thus, during an active session, the transactions can be secured or unsecured, which is indicated by dashed lines for transactions 1222. If full encryption is selected, each transaction between the local PC and the site server is a secured process. Full encryption may slow down the communications between the local PC and the site server because of the extra encryption processing, but provides a secured computing environment. Additionally, a virus check can be performed on files before the upload (and download) from the local PC to the network.

To terminate the session, the user logs out by clicking on a logout (LO) icon 1232 on a virtual desktop 1230. The logout command is sent to servers 1216. In an embodiment, as part of the logout process, servers 1216 execute (or direct execution) of a termination application 1240 which clears the RAM on the local PC 1250 and the hard dish cache so that "ghost" copies of files are destroyed upon termination of the session. Termination application 1240 can reside on the local PC (i.e., as part of the local PC operating system) that is activated by servers 1216.

Virtual Desktop Processes

FIGS. 13A and 13B show a flow diagram that describes an implementation of an embodiment of the virtual desktop of the invention. The flow diagram describes implementation of some of the features recited above. Thus, FIGS. 13A and 13B should only be taken as representative, and not limitation, of the invention.

In FIG. 13A, at a step 1310, the URL website that supports the virtual desktop receives a URL access from one of the local PC. In response, the URL sends its web page and a login window, at a step 1312. Shortly thereafter, the URL

receives, at a step 1314, the login information and compares, at a step 1316, the received login information with the login information stored at the URL for that user. At a step 1318, a determination is made whether the received login information is valid. If the received login information is not valid, an error message is sent to the local PC, at a step 1320, the login window is redisplayed, at a step 1322 (i.e., with the previously entered data removed from the login window fields), and the site server returns to step 1312.

If the login is valid, the session starts at a step 1330. The site server then directs one of the backend server to handle the session with the user. The security mode (e.g., no encryption, partial encryption, or full encryption), as selected by the user or the server, is then set by the server, at a step 1332.

(col. 15, lines 12-66, emphasis added). While Haung discusses HTTP and encryption, this is not the same as teaching Applicants' claimed invention. Haung is completely out of context when compared to Applicants' claimed invention "wherein the administrative web site in response to receiving the HTTP message: decrypts the HTTP message so as to define a decrypted HTTP message; authenticates the decrypted HTTP message

using a signature contained within HTTP message; and if the decrypted HTTP message is authentic, updates the record in the database in response to the alarm information carried in decrypted HTTP message."

(Claim 4, emphasis added). Haung simply does not teach the claimed invention. Furthermore, claim 8, which depends from claim 4 and indirectly from claim 1, is further not obvious for reasons discussed above with respect to each of claims 1 and 4.

Claim 10

Claim 10, depends from claims 1 and recites: "The apparatus in claim 1 further comprising the administrative web site wherein the database contains a plurality of customer records, where each of the plurality of customer records is associated with a corresponding one of a plurality of different SEPs and each of the different SEPs is associated with a different one of a plurality of LANs such that all of said LANs are monitored through the administrative web site." (emphasis added). The Office action at page 6, paragraph 14 states: "As per claim 10, Huang et al teach an administrative web site wherein the database contains a plurality of customer records, where each of a plurality of customer records is associated with a corresponding one of a plurality of different servers and each of the different servers is associated with a different one of a plurality of LANs such that all of said LANs are monitored through the administrative web site

(column 4, lines 35 - 55; records can include correspondence to particular SEP)."

The citations to Haung are repeated as follows for convenience:

Site server 230 couples to, and provides the login information to, a controller server 240. Controller server 240 checks the login information against a database 242 of login information to determine whether the user is authorized for access to the network. If the user is authorized, controller server 240 determines the appropriate Hypertext Transport Protocol (HTTP) server to which the user should be directed. In a large network that includes more than one backend server, controller server 240 directs the user computer system to the appropriate (i.e., the least congested) backend server. In an embodiment, site server 230 and controller server 240 are integrated into one server.

Site server 230 further couples to a bus 244 that interconnects one or more regional networks 250. Each regional network 250 supports a particular geographic area. For example, regional network 250a can cover a geographic area such as the United States and regional network 250n can

cover another geographic area such as Asia.
Within each regional network 250, a number of
backend servers 260 services the assigned
geographic area.

(col. 4, lines 35-55, emphasis added). Applicants' fail to understand the relevance of Haung's "determines the appropriate ... server to which the user should be directed" to their claimed "each of the different SEPs is associated with a different one of a plurality of LANs" which is clearly not the same as Applicants' SEP and is clearly not being used in the context of the claimed invention. Furthermore, Claim 10, which depends from claim 1 is not obvious for reasons discussed above with respect claim 1. Therefore, Applicants respectfully request that the rejection be withdrawn.

Claims 11-12

Regarding claims 11 and 12 which depend directly or indirectly from claim 1, for the reasons given above with respect to claim 1, claims 11 and 12 are not obvious. Therefore, Applicants respectfully request that the rejection be withdrawn.

Claim 13

Claim 13, depends from claims 1 and recites:
"The apparatus in claim 1 wherein the processor, in

response to the stored instructions and if a plurality of alarm messages exists, prioritizes and queues each of the plurality of alarm messages from the SEP for transmission to the administrative web site." (emphasis added). The Office action, at page 7, paragraphs 19-20, states: Huang et al teach the use of an SEP (Figure 2, site server) ... Huang et al fail to teach in response to the stored instructions and if a plurality of alarm messages exists, prioritizes and queues each of the plurality of alarm messages from the a computer for transmission to the administrative web site ...". However, Burgess et al teach tracking of important events on an event queue (Figure 3) occurring on individual computers and forwarding these events to a central monitoring location so that an operator may take action in response to those events according to priority (column 2, lines 54 - 63). It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to combine the teachings of Zhu et al and Burgess et al to Huang et al's apparatus because Zhu et al's use of a monitoring application status and event flags to identify alarm conditions and Burgess et al's use of a database and an event queue in Huang et al's method would allow for a monitoring entity to view alarms organized in an event queue according to priority level in order to take action according to the most urgent event."

The Burgess citation is repeated as follows:
The invention also allows network operators to track important events occurring on individual

computers in the network. The invention forwards these events to a central monitoring location so that a network operator may take action in response to these events. The invention allows filtering of events so that only important events are forwarded to the central location. At the central location, system administrators can gather data from a number of servers in a client/server network. Gathering data in a central location increases the efficiency of system administrators.

(col. 2, lines 54-64, emphasis added). The citation clearly does not teach Applicants' "prioritizes and queues each of the plurality of alarm messages from the SEP for transmission to the administrative web site." Furthermore, Claim 13, which depends from claim 1 is not obvious for reasons discussed above with respect to each of claim 1. Therefore, Applicants respectfully request that the rejection be withdrawn.

Claim 14

Claim 14 depends from claim 1 and recites: "The apparatus in claim 1 wherein the administrative web site downloads to the memory in the SEP a corresponding pre-defined configuration profile which specifies an operational and network environment of the LAN for subsequent use in initializing the SEP." (emphasis added).

The Office action states: "As per claim 14, Huang et al teach administrative website (Figure 4; 420) downloads to memory a corresponding pre-defined configuration profile which specifies an operational and network environment of the LAN for subsequent use in initializing the SEP (column 8, lines 2862)."

The Haung citation is repeated as follows:

The virtual desktop layout and configuration can be tailored to the user's particular preference. Customization of virtual desktop 420 can be initiated by (double) clicking on a customize icon 428 that activates a customize window 438. Customize window 438 includes the tools and features that allow the user to customize the virtual desktop. The operation of the customization feature of the invention is described in further detail below.

FIG. 5 shows a diagram of an embodiment of the data stored for the users in the virtual computing environment. Referring back to FIG. 2, data associated with the users is stored in one or more databases, including user login information database 242, e-mail database 274, user information database 278, and user file database 282. The information associated with each user can be represented by a data

record 510. Data record 510 includes, for example, virtual desktop layout information 512, a list of applications 514 that the user has been authorized for access, files and folders 516, and personal information 518. Additional types of data can be stored for each user. Also, the data size for each data type can vary from user to user based on, for example, a particular user's requirements. The number of files and the total storage area typically vary among users. The number of applications authorized and the amount of available storage space may further be dependent on, for example, payment of a service fee.

Although the data for each user is shown as being integrated to a single data record, the data within the record may, in actuality, be stored in separate databases. For example, the desktop layout information, the list of authorized applications, and the personal information for all users may be stored in user information database 278, and the files and folders may be stored in user file database 282. Alternatively, the entire record may be stored on one database at a central server.

(col. 8, lines 28-62, emphasis added). Applicants have thoroughly reviewed the citation and fail to find any

teaching of Applicants' claimed "a corresponding pre-defined configuration profile ... for subsequent use in initializing the SEP. Certainly the Examiner isn't implying that Haung's mere use of "stored" is teaching Applicants' downloads to the memory in the SEP. Applicants respectfully note that Haung's "stored" does not teach anything about the claimed downloads in the context of the SEP of the present invention. Furthermore, claim 14, which depends from claim 1 is not obvious for reasons discussed above with respect claim 1. Therefore, Applicants respectfully request that the rejection be withdrawn.

Claims 15-16

Regarding claims 15 and 16 which depend directly or indirectly from claims 14 and 1, for the reasons given above with respect to claims 1 and 14, claims 15 and 16 are not obvious. Therefore, Applicants respectfully request that the rejection be withdrawn.

2. § 103 Haung in view of Zhu in view of Rein

The Office action, at paragraph 24, has rejected claims 5-7, 9, 18-20, 22, 28-30, 32, 41-43 and 45 under the provisions of 35 USC § 103 as being obvious over the teachings in Haung taken in view of Zhu and further in view of "Live Data from WDDX by Lisa Rein dated October 6, 1998

Appl. No. 09/835,075
Amdt. dated January 31, 2005
Reply to Office Action of November 5, 2004

(hereinafter Rein). These rejections are respectfully traversed.

Claims 5, 6, 7 and 9

Regarding claims 5, 6, 7 and 9 which depend indirectly from claim 1 and from at least one intervening claim (2, 4, 5, 6 and 8), for the reasons given above with respect to claims 1, 2, 4, 5 and 8, claims 5, 6, 7 and 9 are not obvious. Therefore, Applicants respectfully request that the rejection be withdrawn.

Claims 28-30, 41-43 and 45

Claims 28-30, 41-43 and 45 depend indirectly from claim 1. For the reasons given above with respect to claim 1 and any intervening claim, Applicants respectfully submit that claims 28-30, 41-43 and 45 are not obvious and that the rejection of said claims be withdrawn.

Conclusion

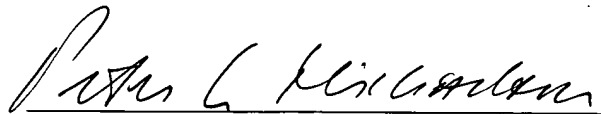
Thus, the Applicant(s) submits that none of the claims, presently in the application, is obvious under the provisions of 35 USC § 103.

Appl. No. 09/835,075
Amdt. dated January 31, 2005
Reply to Office Action of November 5, 2004

Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

Respectfully submitted,

January 31, 2005



Peter L. Michaelson, Attorney
Customer No. 007265
Reg. No. 30,090
(732) 530-6671

MICHAELSON & ASSOCIATES
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

CERTIFICATE OF MAILING under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited on **February 1, 2005** with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to:

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450



Signature



Reg. No.

(NETILLA2AMEND/ca:17)